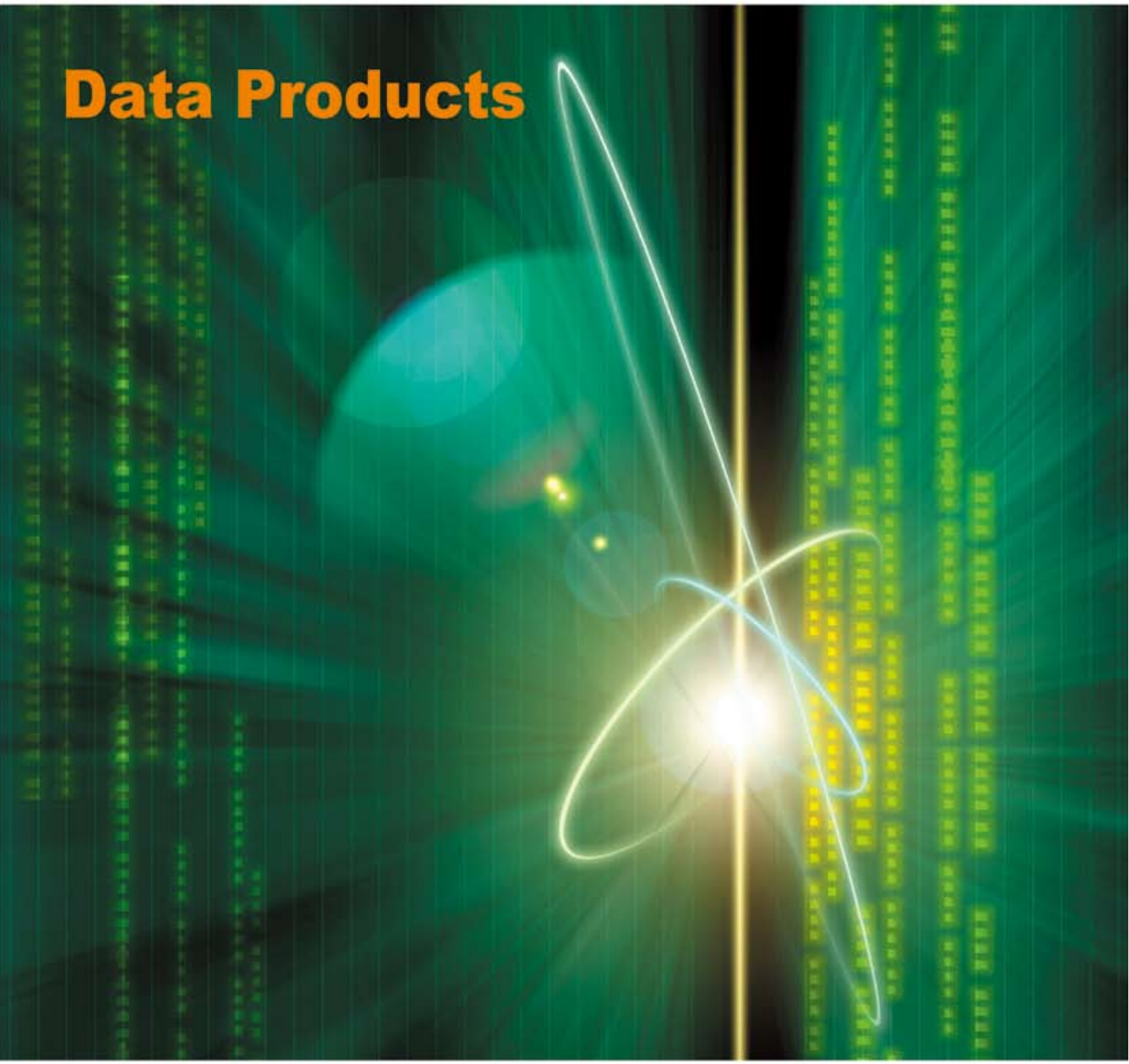
No.33 August 2007 Issue
54

ZTE中兴

Maintenance Experience



Typical Cases
Experience Collection

Preface

In this issue of ZTE's "Maintenance Experience", we continue to pass on various field reports and resolutions gathered by ZTE Engineers and Technicians from around the world.
The content presented in this issue is as below:

- Fourteen Maintenance Cases of ZTE's Data Products

Have you examined your service polices and procedures lately? Are you confident that your people are using all the tools at their disposal? Are they trained to analyze each issue in a logical manner that provides for less downtime and maximum customer service? A close look at the cases reveals how to isolate suspected faulty or mis-configured equipment, and how to solve a problem step by step, etc. As success in commissioning and service is usually a mix of both discovery and analysis, consider using this type of approach as an example of successful troubleshooting investigations.

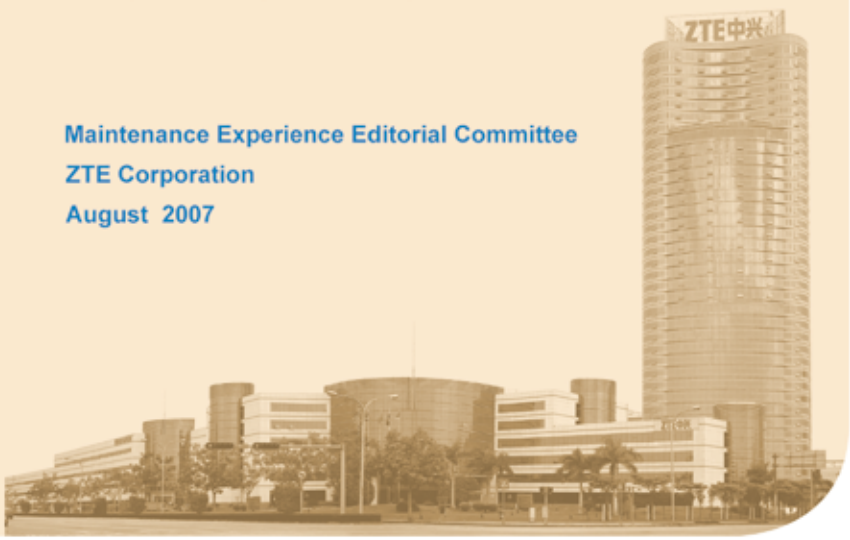
While corporate leaders maintain and grow plans for expansion, ZTE employees in all regions carry out with individual efforts towards internationalization of the company. Momentum continues to build, in all levels, from office interns to veteran engineers, who work together to bring global focus into their daily work.

If you would like to subscribe to this magazine (electronic version) or review additional articles and relevant technical materials concerning ZTE products, please visit the technical support website of ZTE Corporation (http://support.zte.com.cn).

If you have any ideas and suggestions or want to offer your contributions, you can contact us at any time via the following email: doc@zte.com.cn.

Thank you for making ZTE a part of your telecom experience!

Maintenance Experience Editorial Committee
ZTE Corporation
August 2007



Maintenance Experience Editorial Committee

Director: Zhou Susu

Deputy Director: Chen Jianzhou

Editor-in-Chief: Yang Cheng

Editors:

Jiang Guobing, Wang Yaping, Ba Zexue, Zhang Shoukui, Wu Feng, Yuan Yufeng, Tang Hongxuan, Chen Huachun, Ding Guixiang, Gu Yu, Tian Jinhua, Zhu Wensheng, Ling Changwen, Zhang Zhongdong, Liu Xianmin, Wang Zhaozheng, Chen Taiming, Zhang Mingjing, Wang Haidong, Chen Le, Lei Kun, Wang Tiancheng, Zheng Hongliang, Wang Tao

Technical Senior Editors:
Hu Jia,Yu Chengjun,Bai Jianwen

Executive Editors:
Zhang Fan

Maintenance Experience Newsroom

Address: ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzhen, P.R.China

Postal code: 518057

Contact: Song Chunping

Email: doc@zte.com.cn

Tel: +86-755-26770600,26771195

Fax: +86-755-26772236

Contents

02 ARP Attack Troubleshooting
02 Malfunction Situation
02 Malfunction Analysis
03 Solutions
05 Switch Port Self-loop
05 Malfunction Situation
05 Malfunction Analysis
05 Solution
06 ARP Binding
06 Network Topology
06 Malfunction Situation
06 Solutions
08 RSTP Function
08 Building Network Demand
08 Network Topology
08 Solution Selection
09 Solution Implementation
09 Test Results
09 Background Knowledge
11 ACL Configuration
11 Background Knowledge
12 Case 1
12 Malfunction Situation
12 Malfunction Analysis
12 Solution
13 Case 2
13 Malfunction Situation
13 Malfunction Analysis
13 Solutions
14 Case 3
14 Malfunction Situation
14 Malfunction Analysis
14 Solutions
15 Multicast Service
15 Multicasting
15 Equipment and Software
15 Network Topology
16 Test
19 Link Aggregation
19 Background Knowledge
19 Case 1
19 Malfunction Situation
19 Malfunction Analysis
20 Solution
21 Case 2
21 Malfunction Situation
21 Malfunction Analysis
22 Solution
23 802.1x Maintenance Experience
23 Background Knowledge
23 Case 1
23 Network Topology
24 Malfunction Situation
24 Malfunction Analysis
24 Solution
24 Case 2
24 Network Topology
24 Malfunction Situation
24 Malfunction Analysis
25 Solution
26 DHCP Troubleshooting
26 DHCP
26 Malfunction Situation
26 Network Topology
27 Malfunction Analysis
27 Solutions
28 Implementation
29 Lower-End Switch Configuration
29 Preparation
31 Configuration and Reference Command

ARP Attack Troubleshooting

⊙ Wang Tujian, ZTE Corporation

Malfunction Situation

Network center fails to connect to eleven ZXR10 2826 access routers in a student dormitory. 40% users are unable to get online.

Malfunction Analysis

Analysis 1

During Network Management System (NMS) analysis, it is found that 11 switches are virtually disconnected and cannot be successfully pinged from the central equipment room.

Log on to a switch through Hyper Terminal. An IP address of the switch is **172.168.0.123.** It is found that CPU utilization ratio is **93%-100%**. Observe the alarm and configuration information.

Result: No abnormity is found.

Analysis 2

Connect to T40G switch in an assembling layer. It is found that there is a piece of alarm information: too many ARP broadcast packets are received at gei_2/4 interface. Use relative command to show traffic information on the port.

Result: It is found that **100,000** broadcast packets are added in every 10 seconds.

Analysis 3

Analyze the access switch 2826 at gei_2/4 interface. It gives the following causes.

There is a loop at the user side.

User host is toxic and sends broadcast packets continuously.

User installed ARP attack software on host. The host sends broadcast packets continuously.

Result: It is found that 2826 switch has **172.168.0.111** IP address at gei_2/4 interface.

Analysis 4

Connect to the switch again. Break the packets and analyze them.

Result: It is found that there is a host that is sending broadcast packets continuously. MAC address of that host is **00:19:e0:a9:5a: fc.**

Analysis 5

Find the detailed position of the host according to the label. The host is online. Get the host offline.

Result: All ZXR10 2826 switches are now working in a normal way. CPU utilization ratio is below 5%.

Solutions

ARP virus is a popular and easy-burst virus. It caused the following problem in the network: A host was on-line in normal conditions, but all of a sudden it gets off-line and it can not ping its gateway now. Reboot the host and run command **arp –d** in MS-DOS mode. Now the host is on-line for a while.

To solve the problem that is caused by ARP virus, use the following procedures:

- Bind ARP to PC statically.

  Note: It is not suitable for large networks.

1. When the host is on-line, enter into **MS-DOS** mode and input **arp –a** command to observe the correct MAC address that corresponds to a gateway IP address. Now record the MAC address When PC gets failed to get on-line then run **arp –d** command to delete contents in ARP buffer to recover the PC temporarily. Once the PC gets online, get it offline and then run arp –a command.

Example: suppose gateway address of a host is **218.197.192.254.** Host IP address is **218.197.192.1**. When host is online in normal condition then run **arp –a** command that shows the following output:

C:\Documents and Settings>arp –a

Interface: 218.197.192.1 --- 0x2

Internet Address Physical Address Type

218.197.192.254 00-01-02-03-04-05 dynamic

00-01-02-03-04-05 is the MAC address of gateway. It has a dynamic type, so it is possible to change its type.

2. When host can not get online in normal way, bind IP gateway MAC manually. To bind them, run **arp –s <gateway IP> <gateway MAC>** command.

Example: arp –s 218.197.192.254 00-01-02-03-04-05

After binding, use **arp –a** command to view ARP buffer:

C:\Documents and Settings>arp –a

Interface: **218.197.192.1** --- 0x2

Internet Address Physical Address Type:

218.197.192.254 00-01-02-03-04-05 static

Now the type is static. Manual binding is disabled when host is turned off. When host is turned on , it is necessary to perform the binding again.

- Find out the toxic host and clear the virus. It is advised to install special tool on hosts in the whole network.

1. Use **arp –a** command after ARP attack, as a result it is found that gateway MAC is replaced by an attacked host MAC. consider it as **00-01-06-07-08-09.**

C:\Documents and Settings>arp –a

Interface: **218.197.192.1** --- 0x2

Internet Address Physical Address Type:

218.197.192.254 00-01-06-07-08-09 dynamic

Record this MAC address for further solution.

With the recorded MAC address, use **show mac** command to find the port through which the toxic host accesses. Consider that the toxic host is connected with T64 switch. **Use show** mac command. It gives the output, as shown in Figure 1. Isolate the toxic host and clear the ARP virus.

```
ZXR10(config)#show mac
Total mac address : 6
Flags:vid —-VLAN id,stc—static,per—-permanent,toS—-to—-static,
srF  —-source filter,dsF —-destination filter,time —-day:hour:min:sec
Frm —-mac from where:0,drv;1,config;2,VPN;3,802.1X;4,micro;5,dhcp
 MAC_Address   port    vid   static  locked src_filter dst_filter
-------------------------------------------------------------------------------------
0001.0607.0809   fei_8/6    200   0     0        0          0
0000.0000.2222                1      1     1        1          0
0000.0000.0022   fei_8/14  888    0     0        0          0
0000.0000.1111   gei_3/3   888    1     0        0          0
0000.0000.3333   gei_3/3   888    1     1        0          0
0000.0000.0021   fei_8/12  888    0     0        0          0
-----------------------------------------------------------------
ZXR10(config)#
```

Figure 1. The output of the command

2. Install special tool on hosts in the whole network, such as ARP fire-wall. ■

Switch Port Self-loop

⊙ Tu Yong, ZTE Corporation

Malfunction Situation

An organization uses a ZXR10 3928 switch to connect the private line network centers. Switch was working normally until several new private lines are added. Newly added private lines have not started to perform their functions. But CPU utilization ratio of ZXR10 3928 switch is still high, and the primary services are interrupted.

Malfunction Analysis

Observe the equipment. It is found that the switch MAC address is continuously drifting. After close observation, it is found that the switch is connected to network centers through fiber transceiver. As the transceiver has no user as yet, it loops receiving and sending. Port self-loop occurs that causes a problem.

Solution

To solve this problem, perform the following steps:

1. Close the transceiver that has no user.

2. Use a port self-loop detection function on the switch to find out on which port self-loop occurs.

Perform the following steps to use port self-loop detection function on switch:

i. Enable self-loop detection function on a port or multi ports.

```
ZXR10(cfg)#loop-detect interface
```

ii. Set the vlan in which loop detection is enabled.

```
ZXR10(cfg)#loop-detect interface <port-name> vlan <vlan-id> enable
```

iii. Enable loop-detect protection function.

```
ZXR10(cfg)#loop-detect protect-interface <port-name> [enable|disable]
```

If **loop-detect protect-interface** <port-name> **enable** command is configured on switch then a switch does not take any measure after an alarm is sent. If **loop-detect protect-interface** <port-name> **disable** command is configured then a switch closes a port during the loop occurrence. A loop-detection protection function is enabled in this case.

Note: By default, a loop-detection protection function is **disable.** ■

ARP Binding

⊙ Yang Yong, ZTE Corporation

Network Topology

Enable NAT on GAR router to provide public network addresses for internal PCs, as shown in Figure 1. Internal network IP address on GAR is **192.168.2.2.** Vlan1 IP address on ZXR10 3906 is **192.168.2.1.** All users are in Vlan1 and have fixed IP, and their gateway address is **192.168.2.1.**

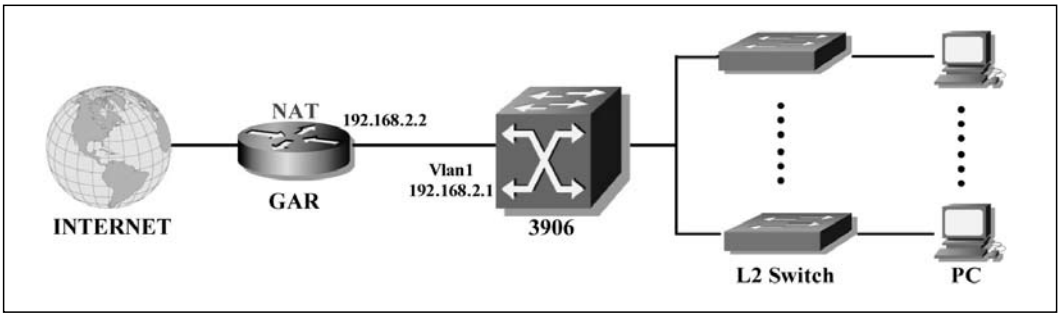


Figure 1. Network Topology of ARP Binding

Malfunction Situation

There are two malfunctions:

- Some users are unable to get online and are unable to ping successfully to gateway.
- Bind an internal network IP to a MAC address to prevent a user to set an IP at random. But binding is not effective in this case.

Solutions

Malfunction 1

Log on to GAR and 3906 to check ARP tables. It is found that there are some items that have the age as TS, as shown in the following content.

Address	Age(min)	Hardware Addr	Interface
192.168.2.70	**TS**	**0090.f547.8112**	**fei_0/1**
192.168.2.157	**TS**	**0015.c577.2b98**	**fei_0/1**
192.168.2.35	**TS**	**0020.eda8.67fd**	**fei_0/1**

It indicates that the users who have the IP addresses are with TS and are not able to get online. MAC addresses of these users do not correspond to the PC MAC addresses.

There are two types of ARP table binding: static and permanent. Ages of the two types are defined as S and P respectively. These items can not be deleted with command **clear arp.**

When searching related ARP commands on GAR and 3906 L3 interfaces, it is found that there are two types of ARP static bindings: dynamic and manual. Manual binding is to use **set static** command to bind MAC and IP. Use **show run** command to view the result, such as **set arp static**

192.168.2.185 0016.ec3f.73c3. Dynamic binding is to use **arp to-static** command to bind IP in an ARP table to MAC in an automatic way. A result can not be viewed with **show run** command.

Note: In an ARP table, TS is referred as "To Static".

Use **clear arp static** command on GAR and 3906 L3 interfaces to clear the static binding. Use **show arp** command to view ARP table, and there are no items with TS. Now the users can get online.

Malfunction 2

IP and MAC addresses are bonded on ZXR10 3906 Vlan1 interface, as shown in the following content.

set arp permanent 192.168.2.185 0016.ec3f.73c3

set arp permanent 192.168.2.173 0015.5820.ba3d

set arp permanent 192.168.2.218 0016.ec3f.689d

After performing the tests, it is found that the binding is not effective. User that has a MAC address such as **0016.ec3f.73c3** can use IP **192.168.2.173** to get online.

After checking the configuration, it is found that there is no problem. Use **show arp** command to view ARP table, it is shown that the internal user IP Age is set as P.

Use **show ip traffic** command. Result shows that there are many ICMP redirect packets on ZXR10 3906 switch. Check the network topology again. Result shows that an internal PC gateway is **192.168.2.2** on internal interface of GAR router, although it is configured as **192.168.2.1** on Vlan1 interface of 3906 switch. There is L2 forwarding but not L3 transmission. ARP binding should be performed on an internal interface of GAR router instead of 3906 switch vlan1 interface.

Use **clear arp permanent** command on 3906 switch vlan1 interface to clear ARP bindings, and then configure bindings on an internal interface of GAR router:

set arp permanent 192.168.2.185 0016.ec3f.73c3

set arp permanent 192.168.2.173 0015.5820.ba3d

set arp permanent 192.168.2.218 0016.ec3f.689d

If an IP address is set as **192.168.2.173** on PC that has a MAC address such as **0016.ec3f.73c3,** then the PC can not ping a gateway.

If a PC IP is set to an address that has no binding IP, such as 192.168.2.254 then the PC can ping a gateway. It is due to a fact that a GAR allows a MAC in ARP table to bind it to IPs, as shown in the following content.

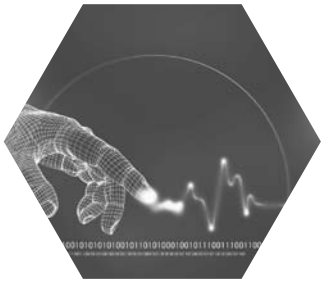
Address	Age(min)	Hardware Addr	Interface
192.168.2.185	**P**	**0016.ec3f.73c3**	**fei_0/1**
192.168.2.254	**2**	**0016.ec3f.73c3**	**fei_0/1**

To prevent this problem, make a spoofing binding to idle IP addresses.

Example: Use the following command:

set arp permanent 192.168.2.254 0000.0000.0000.

Note: Set internal PC gateway to 192.168.2.2. ■



RSTP Function

⊙ Yang Yong, ZTE Corporation

Building Network Demand

There is SS heartbeat detection in two NGN rooms that requires two ZXR10 2826S switches in each room. SS primary heartbeat line connects to one switch, and backup heartbeat line connects to the other switch. This is for equipment and links redundancies and it avoids signal-point malfunction.

Network Topology

Use NO.24 electrical ports to connect the switches in the same room and use NO.25 optical ports to connect the switches in different rooms, as shown in Figure 1. SS heartbeat line is connected to NO.1 electrical port on each switch.

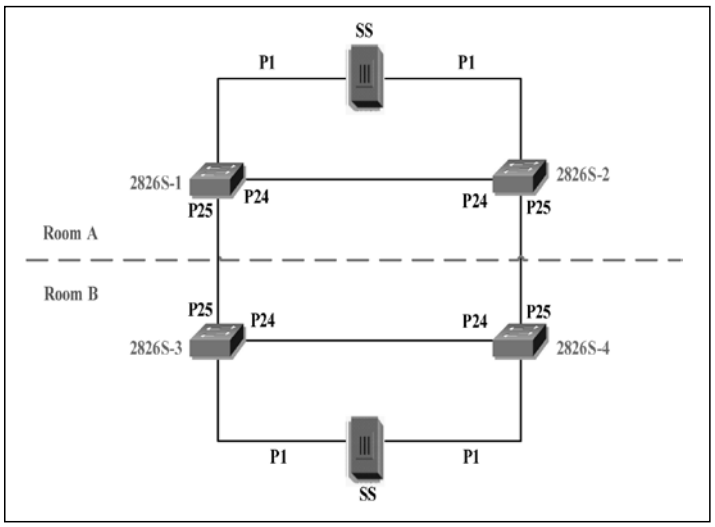


Figure 1. RSTP Topology

Solution Selection

As the four switches are connected in such a way that they form a loop, it is necessary to enable STP to prevent logical loop. ZXR10 2826S switch supports three types of STPs:

- STP
- RSTP
- MSTP

Convergence speed of 802.1d STP is slow (50s). As the network topology is simple and there is no Vlan, it is not necessary to use MSTP. In this case RSTP is suitable.

ZXR10 2826S switch also supports STR reply. STR reply makes the switch that does not allow STP to forward BPDU packets.

There are two solutions:

- Enable RSTP on one switch, and enable STP relay on the other three switches.
- Enable RSTP on the four switches.

If RSTP is enabled on 2826S-1 and STP reply is enabled on the other three switches then the NO.25 port on 2826S-1 has a discard status. NO.24 port is in forwarding status in this case. Data flow from 2826S-1 to 2826S-3 is **2826S-1→2826S-2→2826S-4→2826S-3.**

After performing the tests, it is found that the convergence speed is not good (15s). So use the second solution.

Solution Implementation

For network structure preciseness and maintenance convenience, set each bridge PRI manually to designate a root bridge.

2826S-1 PRI is 4069, 2826S-2 PRI is 4096*3, 2826S-3 PRI is 4096*2, and 2826S-4 PRI is 4096*4. Therefore 2826S-1 in Room A is selected as a root bridge in the network, as shown in Figure 2. NO.24 and NO.25 ports on 2826S-1 are the designated ports for their own segments.

According to STP working principle, NO.25 port on 2826S-4 is in discard status. It discards the frames and does not learn MAC address, so there is no loop in this network.

ZXR10 2826S switch supports edge-port function. Edge-port does not take part in STP. Its status can be from discarded state to a forwarding state. Other ports have **30s** time delay for status transformation from a discarded state to a learning state and then to a forwarding state. Set the ports as edge-ports except NO.24 and NO. 25 ports on each switch to increase the convergence speed.

Configuration is shown in the following content.

```
set stp enable
set stp forceversion rstp
set stp instance 0 bridgeprio <0-61440>
set stp edge-port add port 1-23
set ipport 0 ipaddress 172.16.0.x
255.255.255.0
set ipport 0 vlan 1
set ipport 0 enable
```

Use show stp **(show stp instance 0, show stpport <1-25>)** and **Ping** commands to check whether the switches and ports are consistent with the description in Figure 2 or not.

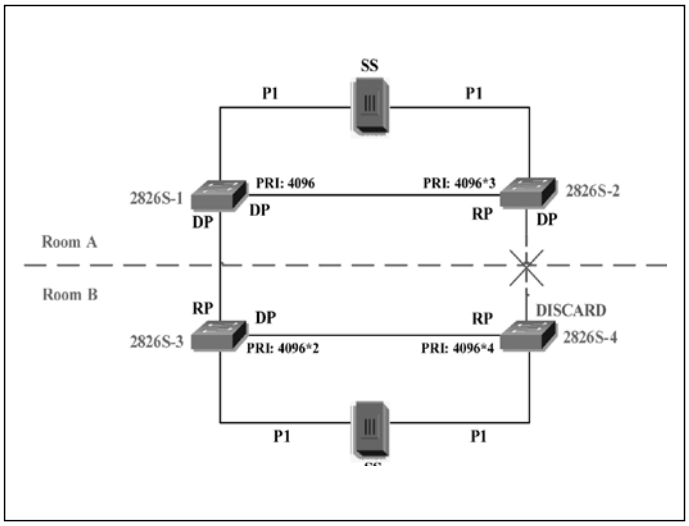


Figure 2. RSTP Implementation

Test Results

Connect a PC to a port on a switch. Set the PC IP to **172.16.0.x/24** and ping the management addresses of the four switches. Then perform the following tests:

- Turn off the switch.
- Turn down the links between switches in different rooms.
- Turn down the links between switches in the same room.

Convergence time of these tests ranges from 0s to 6s. It matches an expected demand.

Background Knowledge

Spanning Tree Protocol (STP) is applicable to a loop network. It blocks the redundant paths via specific algorithm. It changes a loop network into a loop-free tree topology. It is used to prevent the message proliferation and endless cycling in a loop network.

Bridge Protocol Data Unit (BPDU) is used to send STP information between bridges. There are two types of BPDU:

- Configuration BPDU: It is sent by the root bridge every two seconds.
- Topology Change Notification BPDU(TCN BPDU): It is sent to upriver a root bridge by the switch that finds a topology change.

STP performs the following steps to create a loop-free logical topology:

1. Root bridge selection: A switch with the lowest bridge ID becomes the root bridge. A Bridge ID consists of bridge PRI and MAC address. By default, bridge PRI is 32768.

2. Select a root port: A port with the minimum accumulated path cost to root bridge becomes the root port.

3. Select a designated port: A port with the minimum path cost becomes the designated port.

4. Set the redundant switch port as a discard port to avoid loop in topology network.

Port status is shown in Table 1.

STP timers are shown in Table 2.

ZXR10 2826S STP module supports three modes that include SSTP, RSTP and MSTP. These modes comply with IEEE802.1d, IEEE802.1w and IEEE802.1s respectively.

- SSTP (Single Spanning Tree Protocol) fully complies with IEEE802.1d in functionality. A bridge that is running STTP mode can be interconnected with RSTP and MSTP bridges.
- RSTP (Rapid Spanning Tree Protocol) provides higher convergence speed than an STP (i.e. SSTP mode). When a network topology changes, then the status of old redundant switch port is transferred (From Discarded to Forwarded) quickly in the case of point-to-point connection.
- Concepts of instance and VLAN mirroring are added in MSTP (Multiple Spanning Tree Protocol). SSTP and RSTP mode are considered to be MSTP mode instances. Only one instance 0 exists is an example. MSTP mode also provides fast convergence and load balance in VLAN environment.

In SSTP and RSTP modes, there is no VLAN concept. There is only one status for each port that is a forwarding status. This status is consistent in different VLANs. But in MSTP mode, there are multiple spanning tree instances. Forwarding statuses of ports are different in different VLANs. Multiple independent sub-tree instances can be formed inside MST region to achieve load balance. ■

Table 1. Port Status

Status	Action
Blocking	All ports are in this status when switch starts. In this status, a port does not forwarding frames. It detects BPDUs to prevent loop.
Listening	In this status, a port detects BPDUs to judge whether there is a loop before forwarding frames.
Learning	In this status, a port detects BPDUs and learns all paths and MAC tables. It does not forwards frames.
Forwarding	In this status, a port forwards and receives frames.
Disable	In this status, a port does not take part in STP or forward frames. It is administratively closed.

Table 2. STP Timers

Timer	Definition	Interval
Forward Delay	The time for learning and listening.	30s
Max Age	The time for storage BPDU.	20s

ACL Configuration

⊙ Feng Chao,Gu Weiwei,Wei Hui, ZTE Corporation

Background Knowledge

ACL is used to implement the data message filtering, policy routing and special flow control. An ACL may contain one or more rules defined for special types of packets. These rules tell the switch to allow or deny the access of packets that match the criteria specified in the rules.

ZXR10 T160G/T64G/T40G provides seven types of ACLs:

- Basic ACL: Only source IP addresses are matched against the ACL.
- Extended ACL: Source/destination IP address, IP protocol type, TCP source/destination port number, UDP source/destination port number, ICMP type, ICMP code, DiffServ Code Point (DSCP), ToS and precedence are matched against the ACL.
- Layer 2 ACL: Source/destination MAC address, source VLAN ID, Layer 2 Ethernet protocol type and 802.1p priority value are matched against the ACL.
- Mixed ACL: Source/destination MAC address, source VLAN ID, source/destination IP address, TCP source/destination port number, UDP source/destination port number are matched against the ACL.
- Basic IPv6 ACL: Source IPv6 address is matched against the ACL.
- Extended IPv6 ACL: Source/destination IPv6 address is matched against the ACL.
- User-defined ACL: Number of VLAN TAG and offset byte are matched against the ACL.

Each ACL has an ACL code for identification that is a digit. Code ranges of different ACLs are described in the following content.

- Basic ACL: 1~99
- Extended ACL: 100~199
- Layer 2 ACL: 200~299

- Mixed ACL: 300~349
- Basic IPv6 ACL: 2000~2499
- Extended IPv6 ACL: 2500~2999
- User-defined ACL: 3000~3499

To configure ACL, follow these three steps in order:

1. Configure a time range.
2. Define an ACL.
3. Apply the ACL to physical ports.

Case 1

Malfunction Situation

An ACL is applied on ZXR10 T64E router L3 interface to limit users to telnet. For example, allow the hosts in network management room to telnet to log on ZXR10 T64E router and forbid other users.

ACL is defined as follows:

```
acl extend num 101
rule 1 permit 202.98.4.3 0.0.0.0 any eq telnet
rule 2 permit 202.98.4.8 0.0.0.0 any eq telnet
rule 3 permit 202.98.4.30 0.0.0.0 any eq telnet
rule 4 permit 218.37.5.3 0.0.0.0 any eq telnet
rule 10 deny any any eq telnet
rule 11 permit ip any any
```

Fist four users are allowed to use telnet and others are forbidden.

If a user with an IP **219.38.5.3** is allowed to use telnet then add rule 5 permit **219.38.5.3 0.0.0.0 any eq telnet** command in acl **101**.

First four users can perform the telnet now, but the new users are failed.

Malfunction Analysis

Use **show acl 101** command to view configuration. Result is shown in the following content.

```
acl extend num 101
rule 1 permit tcp 202.98.4.3 0.0.0.0 any eq telnet
rule 2 permit tcp 202.98.4.8 0.0.0.0 any eq telnet
rule 3 permit tcp 202.98.4.3 0.0.0.0 any eq telnet
rule 4 permit tcp 218.37.5.3 0.0.0.0 any eq telnet
rule 10 deny any any eq telnet
rule 11 permit ip any any
rule 5 permit tcp 219.38.5.3 0.0.0.0 any eq telnet
```

Note: Rule 5 is after rule 11, not after rule 4.

A system executes the commands in an order. System executes rule 10 to forbid all users to perform telnet. Rule 5 is after rule 10, so user with IP **219.38.5.3** fails to perform telnet.

In an ACL, the number after rule is only an identifier. It has nothing to do with the execution order. System executes rules according to the rule configuration order.

Solution

There are two ACLs:

ACL101:

```
acl extend num 101
rule 1 permit tcp 202.98.4.3 0.0.0.0 any eq telnet
rule 2 permit tcp 202.98.4.8 0.0.0.0 any eq telnet
rule 3 permit tcp 202.98.4.3 0.0.0.0 any eq telnet
rule 4 permit tcp 218.37.5.3 0.0.0.0 any eq telnet
rule 10 deny tcp any any eq telnet
rule 11 permit ip any any
rule 5 permit tcp 219.38.5.3 0.0.0.0 any eq telnet
```

ACL 102:

```
acl extend num 102
rule 1 permit tcp 202.98.4.3 0.0.0.0 any eq telnet
rule 2 permit tcp 202.98.4.8 0.0.0.0 any eq telnet
rule 3 permit tcp 202.98.4.3 0.0.0.0 any eq telnet
rule 4 permit tcp 218.37.5.3 0.0.0.0 any eq telnet
rule 5 permit tcp 219.38.5.3 0.0.0.0 any eq telnet
rule 10 deny tcp any any eq telnet
rule 11 permit ip any any
```

Results of the above mentioned ACLs are different. ACL 101 allows the first four users to perform telnet. ACL 102 allows the first five users to perform telnet. So pay attention when adding ACL rule items.

Case 2

Malfunction Situation

Define a L2 ACL on ZXR10 T64G switch. When the ACL is applied on port, service is interrupted.

L2 ACL is configured in the following way:

```
acl link number 201
rule 1 permit ip ingress 801 0011.110c.5140
0000.0000.0000 egress any
rule 2 permit ip ingress 801 0011.1149.cf96
0000.0000.0000 egress any
rule 3 permit ip ingress 801 0001.0292.308d
0000.0000.0000 egress any
rule 4 permit ip ingress 801 0008.74db.dadf
0000.0000.0000 egress any
rule 5 permit ip ingress 801 0013.2046.b309
0000.0000.0000 egress any
rule 6 deny any ingress any egress any
```

Malfunction Analysis

ACL rules allow only a part of IP packets to get passed. ARP addresses are aged after several minutes. When ping is performed to check the other end then the host sends an ARP requests. But ARP packets are controlled, so host can not ping successfully. As a result the service is interrupted.

Solutions

Add a r**ule x permit arp any any** command before the **deny any** command to solve this problem.

Note: When ACL is used to deny part of flows then it is necessary to use **permit any any** command at the end of rules. Otherwise all flows are denied. By default, **deny any any** command is added at the end of ACL, although it is not possible to view it with **Show** command.

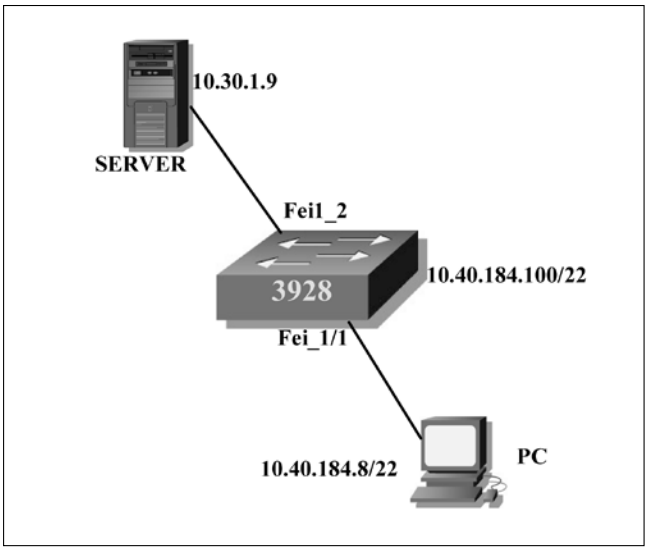


Figure 1. Forbidding Pinging

Case 3

Malfunction Situation

Enable L2 transparent transmission on ZXR10 3928 switch, as shown in Figure 1. Even after applying **deny icmp** command, the PC can still ping the server.

Use **protocol-protect mode icmp disable command to disable** ICMP protection function on the port where ACL is applied. But it fails.

Configuration of ZXR10 3928 is shown in the following content.

```
acl extend number 101
rule 1 deny icmp 10.40.184.0 0.0.3.255 any
rule 2 permit ip any any
!
int fei_1/1
protpcol-protect mode icmp disable
switchport access vlan 1
ip access-group 101 0 in
```

Malfunction Analysis

Integrated format of applying ACL is:

ip access-group <acl-number> <profile-number> **in**

Profile-number is a required parameter. Its value is **0** or **1. 0** means enabling protocol protection. **1** means disabling protocol protection. By default, the value is 0.

Protocol protection is enabled to increase the ICMP PRI by flow table. A flow table is before ACL. ICMP belongs to the content of protocol protection, so its PRI is bigger than ACL.

Configuration on ZXR10 3928 switch uses a default value of profile-number. So ACL is not effective. Now the PC can ping a server.

Solutions

Change the switch configuration as shown in the following content.

```
acl extend number 101
rule 1 deny icmp 10.40.184.0 0.0.3.255 any
rule 2 permit ip any any
!
int fei_1/1
protpcol-protect mode icmp disable
switchport access vlan 1
ip access-group 101 1 in
```

Multicast Service

⊙ Lin Chen, ZTE Corporation

Multicasting

- Multicast Address

Class-D addresses are used as multicast addresses. Multicast address ranges from **224.0.0.0** to **239.255.255.255**.

These addresses have no segment. Any of them can be used as multicast address. Some of them are reserved by system.

  - **224.0.0.0~224.0.0.255**: reserved multicast addresses
  - **224.0.1.0~238.255.255.255**: available multicast addresses for users
  - **239.0.0.0~239.255.255.255**: multicast addresses for local managed or special position

- L2 multicast and L3 multicast
  - In L2 multicast, communication is implemented via switches.
  - In L3 multicast, communication is implemented via routers.
- IGMP

If a switch joins a multicast group, it has to send an IGMP request first. Then it becomes a member to receive multicast messages. A switch should support IGMP Snooping function.

Before enabling IGMP Snooping function, a switch sends multicast messages to every port. After enabling the function, the switch detects IGMP requests. When detecting a request, a switch sends multicast messages to the port. It stops sending multicast messages when it detects leave message.

- PIM

L3 multicast works according to PIM. PIM-SM is the most widely used PIM. It creates a loop-free transmission path from a data source-end to a multi-receive end.

A central point of a PIM-SM group is called Rendezvous Point (RP). Each source sends packets to RP along the shortest-path route and then takes RP as the root node to distribute the packets to all the receivers in the group.

- Multicast routing table

Multicast route is recorded in multicast routing table. The table consists of source address, group address, incoming interface and outgoing interface.

Equipment and Software

Equipment

Redback SE800	version 2.6.5.3
ZXR10 T32C	version 9.4.0.4 NX
ZXDSL 9210	version 3.1.1v

Software

Cisco.IP.TV.Server.v3.4.14-MFD

Cisco.IP.TV.Content.Manager.v3.4.14-MFD

Cisco.IP.TV.Viewer.v3.4.14-MFD

This is IPTV-CISCO kit software. It is used to show multicast service.

Network Topology

Configure two L3 interfaces on T32C-1, as shown in Figure 1. One interface is to connect the multicast source, and the other interface is to connect a BRAS. Configure UNI interface on BRAS to create

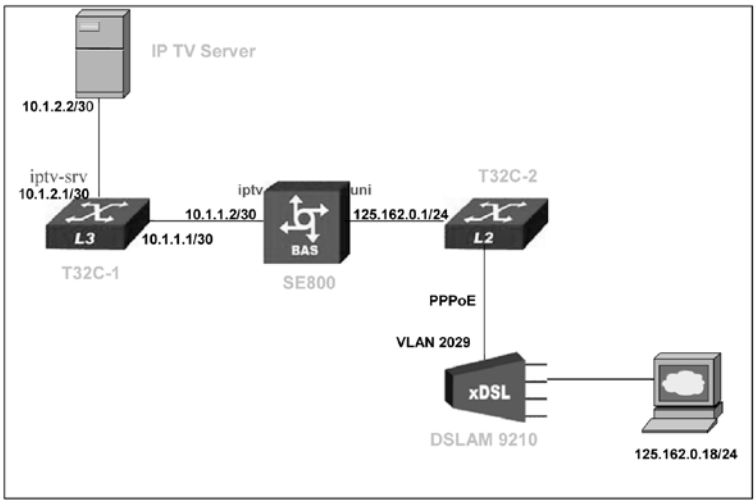


Figure 1. Multicast Network Topology

a connection with PPPoE user on DSLAM. Configure an L2 VLAN on T32C-2.

Configuration on T32C-1

Enable IGMP and PIM SM on interfaces of all routers, from multicast source to receiver. A router should work as RP. Use loopback address or interface address as RP address.

```
T32C-1(cfg)# igmp add interface iptv
T32C-1(cfg)#igmp add interface iptv-srv
T32C-1(cfg)#igmp start
T32C-1(cfg)#pim sparse add interface iptv
T32C-1(cfg)#pim sparse add interface iptv-srv
T32C-1(cfg)#pim sparse static-rp address 10.1.1.1
T32C-1(cfg)#pim sparse start
```

Enable IGMP Snooping function in L2 VLAN. It ensures that the multicast messages are sent to the ports that are added to multicast group.

```
T32C-1(cfg) igmp-snooping add vlan 2029
T32C-1(cfg) igmp-snooping start
```

Configuration on Redback SE800

```
interface iptv
ip address 10.1.1.2/30
pim sparse-mode
interface uni multibind
ip address 125.162.0.1/24
ip pool 125.162.0.0/24
pim sparse-mode passive
```

Enable PIM SM on relevant interface. PIM SM is reliant to IGMP, so it is not necessary to configure IGMP again. Enabling passive PIM SM means that user-end can only receive multicast packets.

Test

Test is considered successful if an image and voice signals can be received. IPTV-CISCO software uses two multicast addresses to transmit image and voice signals, **239.255.0.143** for image signal and **239.255.0.3** for voice signal.

Multicast routing table on T32C-1

```
Medan-T32C-1# pim show routes
PIM Multicast Routing Table
Flags: S - Sparse, C - Directly connected host, L - Local, P - Pruned
R - RP-bit set, T - SPT-bit set
J - Join SPT, F - Directly connected source, E - External join
M - Learned from MSDP, O - MSDP Notified
Timers: Uptime/Expires
Interface state: Interface, Timers, Output Ports
(0.0.0.0/0, 239.255.0.3/32), 04:32:33/never, RP 10.1.1.1, flags: S
Incoming interface: register, RPF nbr (null),
Outgoing interface list:
iptv (10.1.1.1), 00:14:18/00:03:17, gi.4.2,
```

The result above shows a multicast route. It means that this is an RP of a shared multicasting tree. Multicast source can be connected with any interface. Now there is a branch that is going out from interface IPTV.

```
(10.1.2.2/32, 239.255.0.3/32), 00:04:14/00:03:01, flags: STF
Total packet/byte count: 1367/1787971, Rate: n/a
Incoming interface: iptv-srv, RPF nbr 10.1.2.2,
Outgoing interface list:
iptv (10.1.1.1), 00:14:18/00:03:17, gi.4.2,
```

The result above shows a detailed multicast route. It is an instance of shared multicast tree. It means that there is a multicast packet from **10.1.2.2** to **239.255.0.3.** Its next hop is **10.1.1.1**. Incoming interface is **IPTV-srv** and outgoing interface is IPTV.

```
(0.0.0.0/0, 239.255.0.143/32), 04:32:37/never, RP 10.1.1.1, flags: S
Incoming interface: register, RPF nbr (null),
Outgoing interface list:
iptv (10.1.1.1), 00:14:26/00:03:17, gi.4.2,
```

Above result shows shared tree RP of voice signal. Its address is **239.255.0.143/32**. The outgoing interface is IPTV.

```
(10.1.2.2/32, 239.255.0.143/32), 00:04:14/00:03:01, flags: STF
Total packet/byte count: 11014/13693908, Rate: n/a
Incoming interface: iptv-srv, RPF nbr 10.1.2.2,
Outgoing interface list:
iptv (10.1.1.1), 00:14:26/00:03:17, gi.4.2,
```

Above result shows shared tree instance of a voice multicast group. It means that there is a multicast packet from **10.1.2.2** to **239.255.0.143**. Its next hop is **10.1.1.1**. Incoming interface is **IPTV-srv** and outgoing interface is interface **IPTV**.

Multicast routing table on SE800

```
Medan-SE800#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C(c) - Connected(RPF), P - Pruned,
L(l) - Local(RPF), R - RP-bit set, F - Register flag, J - Join SPT,
T - SPT-bit set, m - MSDP learned, H(h) - Static(RPF), V(v) - IGMPv3(RPF),
AW - Assert Winner, AL - Assert Loser, K - state war suppressed,
```

. - No forwarding activity, r - RMR, M - MDT group
Timers: Uptime/Expires
Interface state: Interface, State, Timers, flags
Table version: 282
(*, 239.255.0.143), 00:52:43/00:03:10, RP: 10.1.1.1, Flags: SC
Incoming interface: iptv, RPF neighbor: 10.1.1.1, Next join: 00:00:41
Incoming circuit: 1/3:1023:63/1/1/21
Outgoing interface list:
uni, 2/3:1023:63/1/2/16, Forward, 00:15:31/00:03:10, sparse

Above result shows branch of shared tree. Incoming interface is confirmed. It is **10.1.1.1**. Its outgoing interface is UNI.

(10.1.2.2, 239.255.0.143), 00:05:20/00:01:40, Flags: SC
Incoming interface: iptv, RPF neighbor: 10.1.1.1
Incoming circuit: 1/3:1023:63/1/1/21
Outgoing interface list:
uni, 2/3:1023:63/1/2/16, Forward, 00:05:20/00:03:10, sparse

Above result shows shared tree instance of image multicast group. It means there is a multicast packet from **10.1.1.1** to **239.255.0.143.** Incoming interface is IPTV and outgoing interface is UNI.

(*, 239.255.0.3), 00:52:41/00:03:10, RP: 10.1.1.1, Flags: SC
Incoming interface: iptv, RPF neighbor: 10.1.1.1, Next join: 00:00:41
Incoming circuit: 1/3:1023:63/1/1/21
Outgoing interface list:
uni, 2/3:1023:63/1/2/16, Forward, 00:07:19/00:03:10, sparse

The result above shows shared tree branch of a voice multicast group. Incoming interface of multicast flow is IPTV and outgoing interface is UNI.

(10.1.2.2, 239.255.0.3), 00:05:20/00:01:40, Flags: SC
Incoming interface: iptv, RPF neighbor: 10.1.1.1
Incoming circuit: 1/3:1023:63/1/1/21
Outgoing interface list:
uni, 2/3:1023:63/1/2/16, Forward, 00:05:20/00:03:10, sparse

The result above shows a shared tree instance of voice multicast group. Incoming interface is IPTV and outgoing interface is UNI.

View the Members of the two groups on SE800. **125.162.0.18** is the receiver address. **239.255.0.143** is used to transmit the images, and **239.255.0.3** is used to transmit the voice.

SE800#sh igmp group
IGMP Connected Group Membership
FLAGS: C - Connected, L - Local, V - version 3 connected
Group Address Flags Last ReporterUptime Expires Interface Circuit
239.255.0.143 C 125.162.0.18 00:07:29 00:03:19 uni 2/3:1023:63/1/2/16
239.255.0.3 C 125.162.0.18 00:07:29 00:03:15 uni 2/3:1023:63/1/2/16

Test result shows that the image and voice signals are transmitted in a normal way. ■

Link Aggregation

⊙ Wang Feng,Lan Guotian, ZTE Corporation

Background Knowledge

Theory

Link aggregation technology is also known as trunking. In link aggregation multiple physical ports are combined together and form a single logical port. This implements load balance of in/out flow in each member port. A switch determines the message origin from a member port to the peer end switch according to the port load sharing policy. These policies are configured at user-end.

When a switch detects a broken link in a network then it does not transmit the messages in this particular port until this port link acts normal.

Link aggregation is an important technology in terms of link addition, bandwidth, link transmission, flexibility and redundancy.

ZXR10 T240G/T160G/T64G/T40G supports static Trunk and LACP link aggregation modes.

Static Trunk adds multiple physical ports to trunk group, to form a logical port. This mode goes against observing status of link aggregation port.

LACP

Link Aggregation Control Protocol (LACP) complies with IEEE 802.3 standard. LACP aggregates multiple physical ports to trunk group dynamically via protocol to form a logical port. LACP generates aggregation automatically to obtain the maximum bandwidth.

When configuring link aggregation, pay attention to the following points:

- When the aggregation mode is set as ON then the port runs a static trunk. Two ends that participate in an aggregation must have ON mode.
- When aggregation mode is active or passive, the port runs LACP. Active means that the port is in an active negotiation mode. Passive means that the port is in passive negotiation mode. When configuring dynamic link aggregation, set the aggregation mode of one end of port to be **active** and the other end to be **passive** or set both ends as **active**.
- Link aggregation on ZXR10 T240G/T160G/T64G/T40G supports six types of load balance. They are source IP based, destination IP based, source and destination IP based, source MAC based, destination MAC based and source and destination MAC based. By default, it is source and destination MAC based.

Case 1

Malfunction Situation

A bureau enables the link aggregation between two routers, as shown in Figure 1. As the routers at both ends have no gigabit optical interfaces, the routers are connected via electrical-optical converters.

Link between the router and converter is a twisted-pair, while the link between

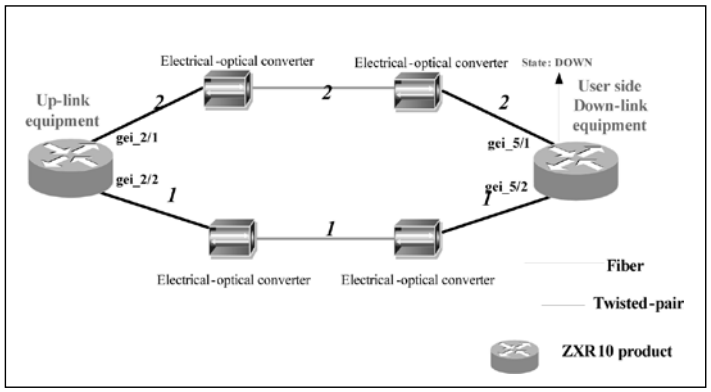


Figure 1. Link Aggregation Topology 1

converters is an optical fiber.

Users that are connected with down-link equipment observe the interruption in some services.

Malfunction Analysis

After checking the equipment and links, the following conclusive points are made:

- Two routers use static trunk to aggregate links.
- A link that is connected to up-link router at user side is down.

A link is connected with up-link router at user side is down; therefore all the up-service flows are shifted to the other link. Interrupted services have something to do with down service flows.

Log in to the router. It is found that the router is still sending the packets to both the links. Routers at both ends use static trunk mode to butt joint, and they are exchanged with the converters. In static trunk mode, as long as the interface is up, interface is one member of the aggregation group.

A destination is a default transmission mode; therefore some packets are sent to the router at user side through path 1, and some through path 2. So some services are interrupted.

Solution

To solve this problem, recover the link, or use LACP mode to butt joint.

To use LACP mode, configure the router as shown in the following content.

```
//create a Trunk//
ZXR10_A(config)#interface smartgroup10
//bind interfaces to Trunk //
ZXR10_A(config)#interface gei_5/1
ZXR10_A(config-if)#smartgroup 10 mode active
ZXR10_A(config)#interface gei_5/2
ZXR10_A(config-if)#smartgroup 10 mode active
//modify VALN link type on smartgroup //
ZXR10_A(config)#interface smartgroup10
ZXR10_A(config-if)#switchport mode trunk
ZXR10_A(config-if)#switchport trunk <vlan-id>
ZXR10_A(config-if)#switchport trunk native <vlan-id>
```

Configuration on up-link router:

```
//create a Trunk//
ZXR10_A(config)#interface smartgroup10
//bind interfaces to Trunk //
ZXR10_A(config)#interface gei_2/1
ZXR10_A(config-if)#smartgroup 10 mode active
ZXR10_A(config)#interface gei_2/2
ZXR10_A(config-if)#smartgroup 10 mode active
//modify VALN link type on smartgroup //
ZXR10_A(config)#interface smartgroup10
ZXR10_A(config-if)#switchport mode trunk
ZXR10_A(config-if)#switchport trunk <vlan-id>
ZXR10_A(config-if)#switchport trunk native <vlan-id>
```

Case 2

Malfunction Situation

ZXR10 T64G is connected to HW 8505 via different 100M equipments, as shown in Figure 2. Links between them are aggregated. It is required to implement load balance on these two links.

When observing flows, it is found that downstream flows (from HW 8505 to ZXR10 T64G) are balanced. Upstream flows (from ZXR10 T64G to HW 8505) are not balanced and all flows go through one link. Make the link through flows go down. Then flows go through the other link. If recovering the link, flows go back through the primary link.

Malfunction Analysis

Aggregation mode is **Manual** on HW 8505, when the links are aggregated. It is advised to use static trunk on HW 8505. As version of HW 8505 is low, it only supports **Manual** mode. System has to be upgraded to use static mode.

For some reasons, HW 8505 up-gradation gets failed. In these circumstances, use **on, active** or **passive** mode on ZXR10 T64G to aggregate the links.

After performing some tests, T64G can only butt joint HW 8505 in **on** mode if HW 8505 uses **manual** mode.

Configuration on T64G is shown in the following content.

```
interface smartgroup1
ip access-group 100 in
switchport access vlan 5
switchport qinq normal
interface fei_2/43
description to 8505
negotiation auto
ip access-group 100 in
switchport access vlan 5
switchport qinq normal
smartgroup 1 mode on
!
interface fei_2/44
description to 8505
negotiation auto
ip access-group 100 in
switchport access vlan 5
switchport qinq normal
smartgroup 1 mode on
```

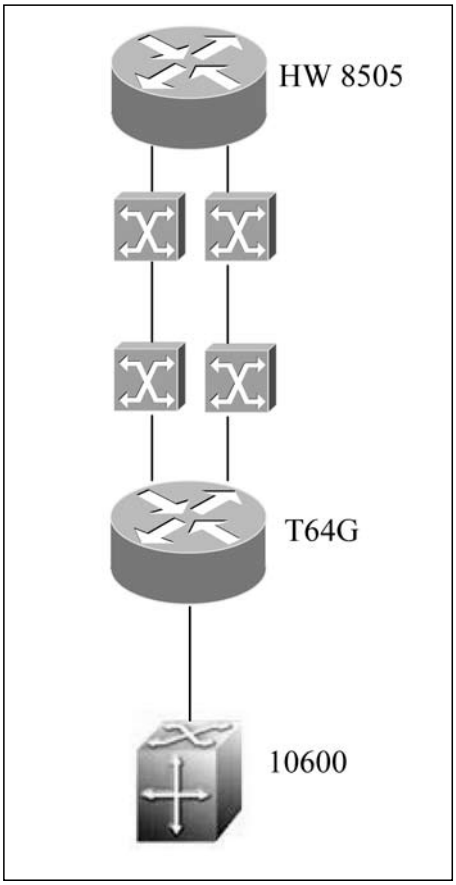


Figure 2. Link Aggregation Topology 2

After troubleshooting, it is found that downstream flows should be balanced by HW 8505 and upstream flows should be balanced by T64G. Now upstream flow

balance fails. It means problem appears onT64G.

After checking T64G configuration, no problem is found. Flows are balanced when both T64G and HW 8505 are in **on** mode.

Use optional commands in interface **smartgroup1** configuration mode. Use **smartgroup load-balance src-dst-ip** command. Now the, upstream flows are balanced successfully.

Solution

When both T64G and HW 8505 are in **on** mode, it is not necessary to add relevant load-balance command manually. When HW 8505 is in **manual** mode, the command should be added manually on T64G.

Configuration on T64G is shown in the following content.

```
interface smartgroup1
ip access-group 100 in
switchport access vlan 5
switchport qinq normal
smartgroup load-balance src-dst-ip
interface fei_2/43
description to 8505
negotiation auto
ip access-group 100 in
switchport access vlan 5
switchport qinq normal
smartgroup 1 mode on
!
interface fei_2/44
description to 8505
negotiation auto
ip access-group 100 in
switchport access vlan 5
switchport qinq normal
smartgroup 1 mode on
```

802.1x Maintenance Experience

⊙ Zhang Jintao,Luo Xiang, ZTE Corporation

Background Knowledge

802.1x is a port based network access control protocol. Its specifications are given by IEEE. Port based network access control is to authenticate and control the equipment access to ports on access control equipment in LANs.

If user equipment that connects to ports can pass authentication then users can visit resources in LANs.

802.1x authentication has the following three parts:

- Supplicant system: PCs request to access the network.
- Authenticator system: switches that support 802.1x.
- Authentication server system: RADIUS servers.

802.1x authentication procedures are as follows:

1. Supplicant system sends EAPOL packets to authenticator system.
2. Authenticator system transmits EAPOR packets to authentication server system.
3. Authentication server system sends EAPOR packets back to authenticator system.
4. Authenticator system sends EAPOL packets back to supplicant system, and decides whether to provide network services for supplicant system or not according to the authentication result.

Case 1

Network Topology

Run ZXISAM authentication software on PC, as shown in Figure 1. Enable 802.1x authentication on ZXR10 2626 switch ports. Run DHCP server on T64G. RADIUS server gateway is on T64G. Configure a network management IP on 2626 switch, and its gateway is on T64G. When supplicant passes authentication, it obtains IP address via DHCP to connect with the network.

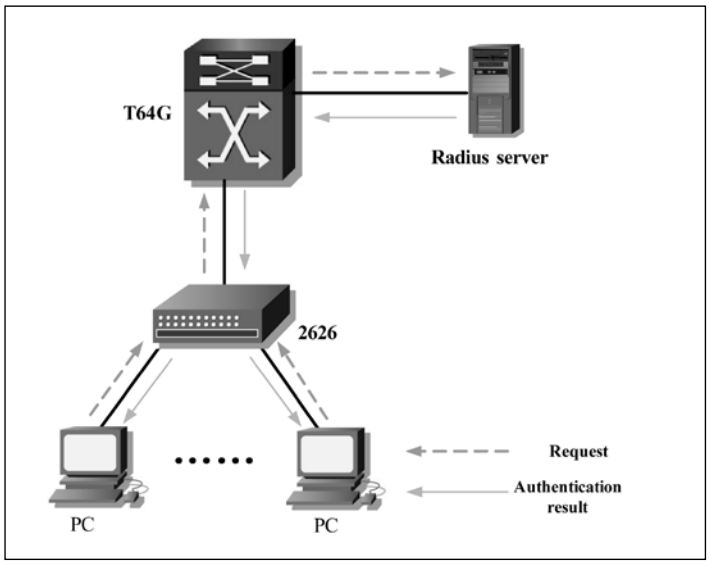


Figure 1. Authentication Topology 1

Malfunction Situation

PC passes authentication and gets online in a normal way. When PC is restarted then it fails to pass authentication.

Malfunction Analysis

When PC fails to pass authentication, it is found that 2626 switch can not ping successfully to its gateway.

Observe ARP table on T64G. It is found that T64G can not learn 2626 switch ARP.

As a result user failure to pass authentication is caused by uneven link between authenticator system (2626 switch and T64G) and authentication server system.

Solution

Bind 2626 switch ARP table item on T64G statically. Then 2626 switch can ping successfully to its gateway on T64G. It can also ping the RADIUS server. PC passes an authentication test and gets online in a normal way.

Case 2

Network Topology

A campus is divided into area A and Area B, as shown in Figure 2. Area A is for teaching and Area B is for student department.

Telecom fiber is connected to a fire-wall and fire-wall is connected to a GER router. In each area, there is a T160G that works as a core switch. It is connected to GER. Several T40G switches are connected to T160G as distribution layer switches. One Hundred 2826S switches are connected to T40G as access layer switches.

Malfunction Situation

802.1x authentication is enabled on 2826S ports. Among 2826S switches that are connected with the same T40G, some of the users that are connected with 2826S switches can pass the authentication and some can not.

A reason impelled on supplicant system is an authentication timeout.

Malfunction Analysis

When checking 2826S switches that pass

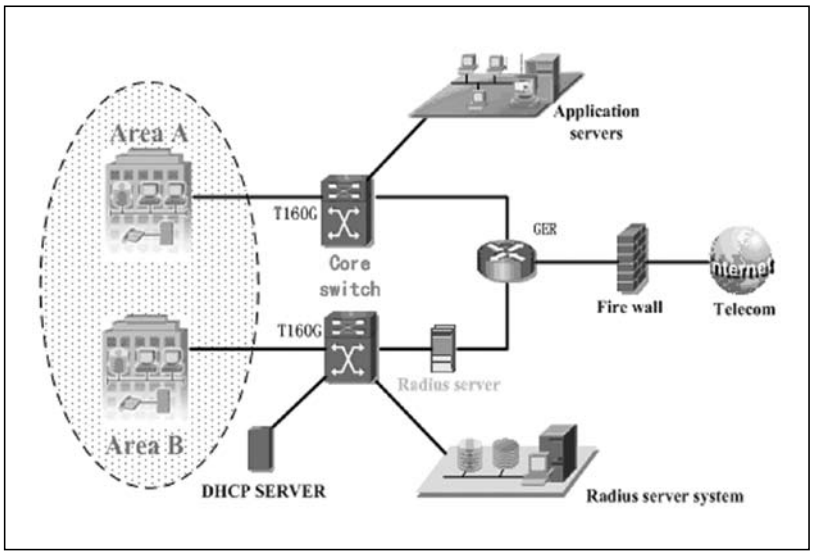


Figure 2. Authentication Topology 2

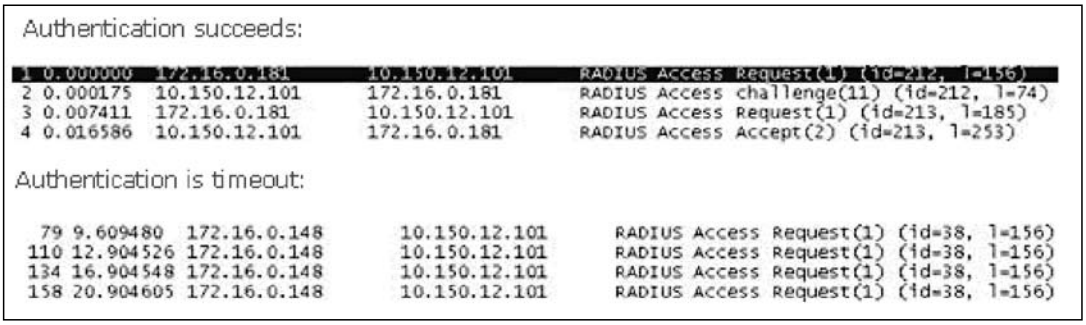


Figure 3. Sniffed Packet Information

authentication and do not pass authentication, it is found that configurations on these switches are the same and the versions are the same.

When sniffing packets, it is found that EAP protocol flow is not finished between 2826S and RADIUS server. Sniffed packet information is shown in Figure 3.

It shows that RADIUS access requests are sent by 2826S switches and are not responded by RADIUS server. So authentication times out.

Observe the RADIUS server logs. It is found that there are many prompts: AP does not support user auth type.

Check the RADIUS configuration. It is found that on some 2826S switches, a shared RADIUS key “amtium” is written as “antium” by mistake. This error stops the RADIUS server to respond.

Solution

Change all the shared keys to “amtium”.

Note: Another useful method to analyze this network problem is to use a packet sniffing tool. ■

DHCP Troubleshooting

⊙ Zhang Fan, ZTE Corporation

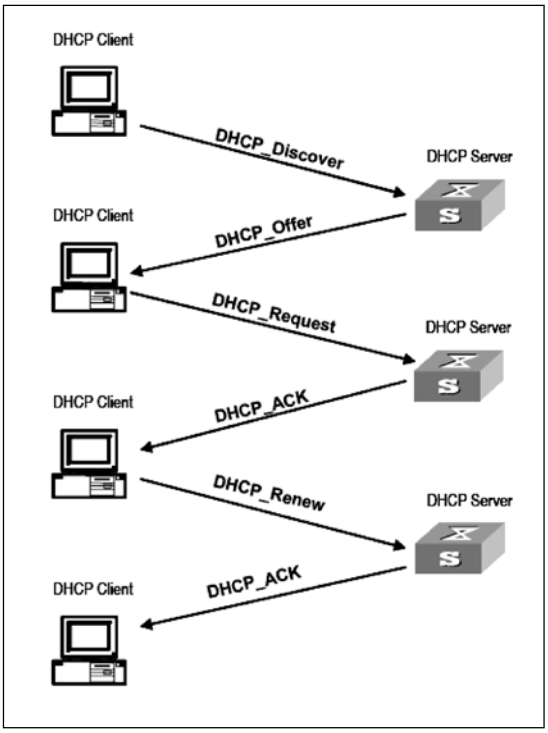


Figure 1. Session Establishment Course

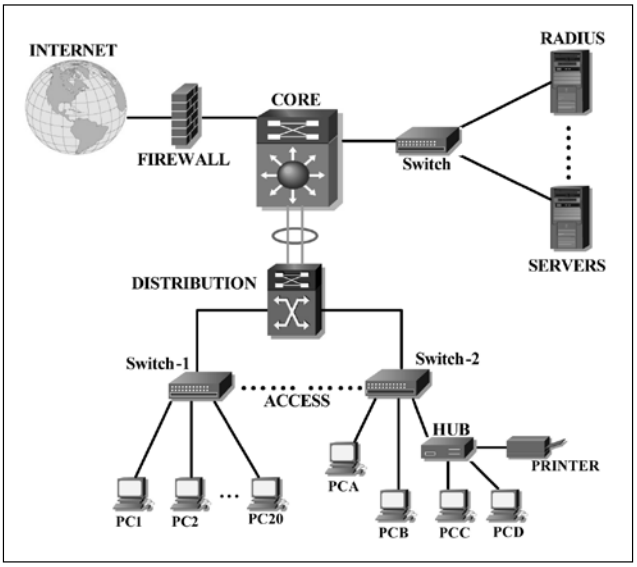


Figure 2. DHCP Topology

DHCP

Background

Dynamic Host Configuration Protocol (DHCP) service is used widely, especially in Ethernet based networks. DHCP does not require IP address, gateway, mask and DNS distribution for every host manually. A host gets the information through DHCP server interaction. Information validity is ensured with lease and continuation mechanism.

After a successful session establishment, a host (DHCP client) gets the service from DHCP Server. Session establishment course between DHCP client and DHCP server is shown in Figure 1.

DHCP decreases preceding configurations for network administrator dramatically. On the other hand it causes some problems that are described in the following section.

Malfunction Situation

DHCP is configured in a campus LAN. Hosts in the LAN obtain IP addresses automatically. After a short while, the following problems appear:

- Some users can not get online from time to time.
- Some users can not get online for a period of time.
- Some users can get online in a normal way.

Network Topology

It is found that the problems appear among users that are connected to a L3 switch at distribution layer, as shown in Figure 2.

A switch in distribution layer works as a DHCP server and a multi–VLAN gateway. Problems exist in multi–VLAN.

Users have to pass web-based authentication to get

online in normal conditions and are charged by time.

Malfunction Analysis

1. After performing RADIUS server diagnosis, no problem is found. Majority of the users have passed the authentication and are charged in a normal way. It shows that the problem is not caused due to RADIUS.

2. Users that are connected to other switches at distribution layer can go online in a normal way. So it is observed that the malfunction lies in the topology, as shown in Figure 2.

3. Log on to the switch to check the configuration. Configuration is the same with other switches in distribution layer. View an ARP table that shows multiple illegal IP address. Normal segment is **10.10.1.X/24**. But there are illegal addresses that belong to a segment **192.168.0.X/24**. Users with these addresses can not get online. As the switch works as DHCP server and the addresses are distributed by this server are in segment **10.10.1.X/24**, it is confirmed that there is no problem in DHCP server.

4. Use **ipconfig** command on a host that can not get online to view its address. It is in segment **192.168.0.X/24**. Change it to an illegal address manually so that it gets online.

5. Spare the addresses and make the hosts to obtain the addresses automatically. Repeat these tests for few times. Results shows that automatically obtained addresses are either in a segment **192.168.0.X/24** or in a segment **172.16.X.X/16**.

Conclusion:

Now it is confirmed that there is at least one illegal DHCP server in a segment. These DHCP servers provide service to users in the segment together with the legal servers.

These problems are solved in the following section.

Solutions

1. Find out the illegal DHCP server position. Use a host with an IP address in segment **192.168.0.X/24**. It is found that its gateway is **192.168.0.1** and it can be pinged successfully from the gateway. It is confirmed that the host that has an IP address **192.168.0.1** is an illegal DHCP server.

Log on to the illegal server to find the network agent software that is running on the host. DHCP function is included in this software. Two IP addresses are bonded to the host. Host is being used as an agent server that distributes the addresses to other hosts. In this situation other users are not charged for being online.

2. There are still some users who are unable to get online. IP addresses are in a segment **172.16.X.X/16.** View an ARP table on switch at distribution layer to find L2 physical access port. It is found that a hub is connected to a port in another room. In the room, there are Four PCs and a printer. No agent software is found on PCs. IP addresses that are obtained on PCs can be illegal or legal.

3. Turn down all the links to the hub. Connect a PC with the hub and then test this PC. Now perform the same tests on the other three PCs. All PCs are working normally. Connect the printer with the hub and then perform a test. It is found that some PCs obtain illegal addresses and a printer is working as a DHCP server.

Printer user manual explains that it enables DHCP server in a segment **172.12. X.X/16** by default to provide service for on-line print. Disable DHCP server function of

the printer with printer client management software and then perform a test. All the PCs obtain legal addresses.

All the problems are solved till now. Two important causes are found:

- Agent software is used illegally.
- Wrong attributes are inserted during the equipment operation.

Implementation

According to the above analysis, enable DHCP Snooping function in a network that has DHCP service. This function prevents the illegal DHCP server effect on the normal and legal DHCP servers.

As a legal server, DHCP server1 is set by network administrator, as shown in Figure 3. It is connected to fei_1/1 interface on switch. DHCP server2 is privately set by users. It is connected to fei_1/2 interface on the switch. Both fei_1/1 and fei_1/2 interfaces belong to vlan100. Enable DHCP Snooping function on switch to prevent illegal DHCP servers affecting normal DHCP servers.

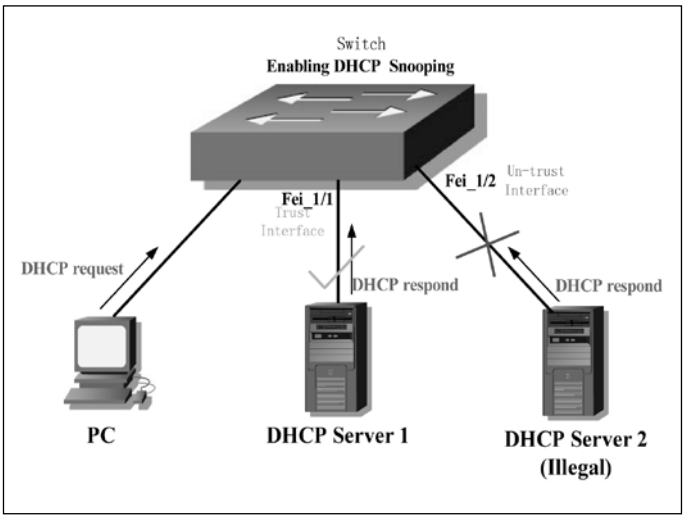


Figure 3. DHCP Snooping

It is necessary to enable DHCP Snooping function in vlan100 and set fei_1/1 as trusted interface. Packets from trusted interface are legal packets. Packets from un-trusted interface are considered as illegal and are discarded.

Configuration on switch:

```
ZXR10(config)#interface fei_1/1
ZXR10(config-if)#sw ac vlan 100
ZXR10(config)#interface fei_1/2
ZXR10(config-if)#sw ac vlan 100
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#ip dhcp snooping trust fei_1/1
```

DHCP function prevents users setting the static IP address and forces the hosts to obtain addresses that are provided by DHCP. It is necessary to use DHCP snooping and dynamic ARP inspection to forbid the static addresses.

Configuration is shown in the following content.

```
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#ip ARP inspection vlan 100
```

Lower-End Switch Configuration

⊙ Lu Jiancheng, ZTE Corporation

Preparation

1. Connect console cable RJ45 joint to console interface at ZXR10 switch front panel.
2. Connect console cable RS232 joint to console interface on PC.
3. Open the Hyper Terminal, as shown in Figure 1. Input the connection name, such as ZXR10, and select an icon.

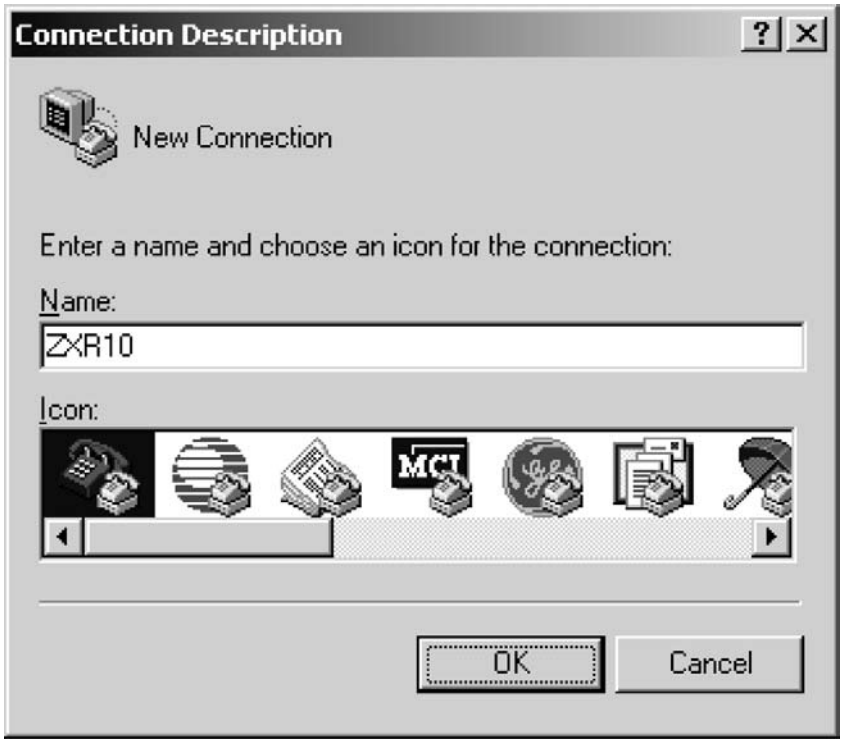


Figure 1. Hyper Terminal Configuration 1

4. Click **Ok**, the window appears, as shown in Figure 2. Select **COM1**, as shown in Figure 2.

Figure 2. Hyper Terminal Configuration 2

5. Click **Ok**, the COM port attribute setup window appears, as shown in Figure 3.

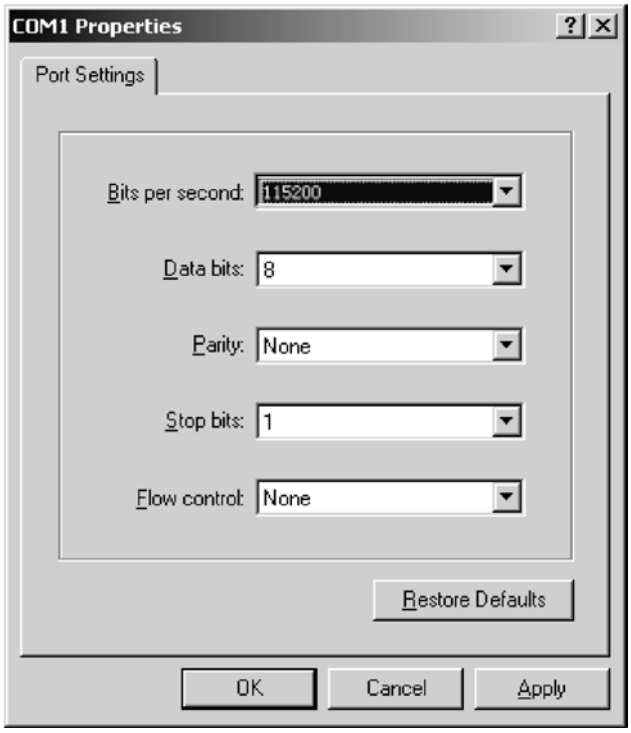


Figure 3. Hyper Terminal Configuration 3

Hyper Terminal COM port has the following settings: "**115200**" for data rate, "**8**" for data bit, "**None**" for parity check, "**1**" for stop bit, and "**None**" for flow control.

6. Click **Ok** to complete the settings. ZXR10 switch configuration window appears. Now start the command operations.

7. Input username as **admin** and password as **zhongxing**. Input **enable** and press **Enter**. Input password as **zhongxing** to enter global configuration mode. The prompt is zte(cfg)#.

Note: On ZXR10 low-end switch, default value of username is **admin** and password is **zhongxing**. Enable password is **zhongxing**.

Configuration and Reference Command

1. Enter the following command to set the hostname.

```
zte(cfg)#hostname zte      //set hostname to zte
```

2. Enter the following commands to create remote login.

```
zte(cfg)#create user zte        //username for remote login is zte
zte(cfg)#loginpass zte      //password for remote login is zte
zte(cfg)#adminpass zte      //enable password is zte
```

3. Enter the following commands to configure the port negotiation.

```
zte(cfg)#set port 1 duplex full
zte(cfg)#set port 1 speed 100
zte(cfg)#set port 1 auto enable    //optical
```

4. Enter the following commands to configure a VLAN.

```
zte(cfg)#set vlan 2 enable
zte(cfg)#set vlan 100 enable
```

5. Enter the following commands to configure uplink port VLAN.

```
zte(cfg)#set vlan 100 add port 1 tag
zte(cfg)#set vlan 2 add port 1 tag
```

6. Enter the following commands to configure user port VLAN.

```
zte(cfg)#set vlan 2 add port 2-24 untag
zte(cfg)#set port 2-24 pvid 2
```

7. Enter the following commands to configure switch management IP.

```
zte(cfg-router)#config router
zte(cfg-router)#set ipport 0 ipaddress 172.32.240.254 255.255.255.0P
zte(cfg-router)#set ipport 0 vlan 100
zte(cfg-router)#set ipport 0 enable
zte(cfg-router)#iproute 0.0.0.0 0.0.0.0 172.32.240.1
zte(cfg-router)#exit
```

8. Enter the following commands to configure an SNMP.

```
zte(cfg)#config snmp
zte(cfg-snmp)#create community zte private
zte(cfg-snmp)#create view zteview
zte(cfg-snmp)#set community zte view
```

AllView

zte(cfg-snmp)#set traphost 10.40.92.105 zte

zte(cfg-snmp)#exit

9. Enter the following commands to configure the isolated ports.

zte(cfg)#set pvlan session 1 add promiscuous-port 1

zte(cfg)#set pvlan session 1 add isolated-port 2-24

10. Enter the following commands to configure L2 multicast.

zte(cfg)#set igmp snooping enable

zte(cfg)#set igmp snooping add vlan 2

11. Enter the following command to limit the user port speed.

zte(cfg)#set port 2-24 bandwidth egress on rate 1000

12. Enter the following commands to limit the user port broadcast packets.

zte(cfg)# set port 2-24 bandwidth ingress on rate 500

zte(cfg)# set port 2-24 ingess_limit_mode broadcast

13. Enter the following command to limit the user port MAC learning.

zte(cfg)#set port 2-24 macaddress 1

14. Enter the following command to describe a port.

zte(cfg)#set port 1 description uplink-to-XXX

15. Enter the following command to name a VLAN.

zte(cfg)#create vlan 100 name guanli

16. Enter the following commands to save the switch configuration.

zte(cfg)#save

zte(cfg)#exit ■

ZTE中兴 ZTE CORPORATION

Add: A Wing, ZTE Plaza, Hi-Tech Road South,
Hi-Tech Industrial Park, Shenzhen, P.R.China
Tel: +86-755-26770000
Postcode: 518057
http://www.zte.com.cn
http://support.zte.com.cn